

WHAT IS CLAIMED IS:

1 *Sub* 1. An apparatus for facilitating the high speed
2 transfer of data to authorized users over the internet, the
3 apparatus comprising:

4 a plurality of host machines for running a plurality of
5 processes;

6 at least one secure communication link between the host
7 machines;

8 a file storage system having a storeroom area and a
9 customer account area with a hard linking capability there
10 between;

11 a firewall with at least one secured host machine
12 residing on the secured side of the firewall; and

13 a customer account database located on the secured host
14 machine and accessible by a secured communication link
15 through the firewall.

1 2. The apparatus of Claim 1, wherein the at least one
2 secure communication link utilizes a protocol for the
3 exchange of arbitrary sized packets of ascii data, delimited
4 by carriage return and newline boundary markers.

1 3. The apparatus of Claim 2, wherein at least one
2 secure communication link enhances the protocol by utilizing
3 DES encryption with N DES keys, and a method for securely

4 passing the DES keys comprising the steps of:

- 5 (i) finding the port number P used for the connection;
6 (ii) computing a value $I = P \text{ modulo } N$; and
7 (iii) using I as the index into the N keys, and using
8 the DES key residing at index I to encrypt and decrypt the
9 data stream.

1 4. The apparatus of Claim 3, wherein the DES
2 encryption creates a cypher string, and a filter is applied
3 to render the cypher string at least 7-bit safe.

1 5. The apparatus of Claim 1, wherein the hard linking
2 capability includes a change root command.

1 *Sub A2* 6. The apparatus of Claim 1, wherein the secured link
2 through the firewall utilizes tobj protocol.

1 7. The apparatus of Claim 1, wherein at least one host
2 machine runs a web server process and at least one separate
3 host machine runs an ftp server process, whereby a customer
4 web browser contacts the host machines.

1 8. A method of facilitating the high speed transfer of
2 data to authorized users over the internet, the method
3 comprising the steps of:

4 (i) running a web server process on at least one host
5 machine;

6 (ii) running an ftp server process on a separate host
7 machine;

8 (iii) establishing a secure communication link between
9 the host machines;

10 (iv) establishing a hard link between storeroom file
11 storage areas and customer account file storage areas; and

12 (v) dynamically allocating customer access information
13 from a secured database.

1 9. The method of Claim 8, wherein step (iii) uses a
2 protocol for the exchange of arbitrary sized packets of ascii
3 data delimited by carriage return and newline boundary
4 markers, and using DES encryption with N keys, step (iii)
5 including the following steps:

6 (a) finding the port number P used for the
7 connection;

8 (b) computing an index value I, where $I = P \text{ modulo } N$; and
9

10 (c) using the DES key residing at index I to
11 encrypt and decrypt the data stream.

1 10. The method of Claim 9, wherein the DES encryption
2 creates a cypher string, and filtering is applied to render
3 the cypher string at least 7-bit safe.

1 11. An apparatus for facilitating the high speed
2 transfer of data to authorized users over the internet, the
3 apparatus comprising:

4 a plurality of host machine means for running a
5 plurality of processes;

6 at least one secure means for communicating between the
7 host machines;

8 a file storage means having a storeroom area and a
9 customer account area with a means for securely hard linking
10 between the areas;

11 a firewall means for providing security between
12 machines; with at least one secured host machine means
13 residing on the secured side of the firewall;

14 a means for databasing customer accounts located on the
15 secured host machine means and accessible by a secured means
16 for communicating through the firewall.

add A³